Context-Aware Intrusion Detection and Tolerance in MANETs

R.S.Ambili Chandran and S.Mary Saira Bhanu

***Abstract*—Mobile ad-hoc network (MANET) is a decentralized network where each node will forward the data to other nodes. The major challenge in handling security in MANETs is that the network is not constant and thereby it is difficult to set a constant algorithm for detecting the intrusion. In this work, a context-aware intrusion detection and tolerance module for MANETs is proposed. A node in MANET can be a filtering node or a monitor node. The intrusion detection based on context awareness is done with the help of filtering and monitoring nodes and intrusion tolerance is done with the help of membership policy. The filtering nodes have minimum level of static database and the monitoring nodes have a database with learning capability. For tolerance, the nodes which are not a member are denied service while the nodes which are members are allowed the service according to some specific rules.**

***Index Terms*— Context-aware, MANET, Intrusion Detection, Intrusion Tolerance**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network of mobile devices connected by wireless links with self- maintenance capabilities. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each of the nodes must forward traffic unrelated to its own use, and therefore be a router. MANETs have limited computational power, memory, communication bandwidth and most important of all energy reserve.Context-awareness deals with linking changes in the environment with computer systems, which are otherwise static. Context-awareness in mobile environment is adaptation to the current situation of the user. The goal is to support the user without too much interaction with a computing device.

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Existing security mechanisms used to protect general computer and network systems are too resource-intensive to be applicable and do not directly apply to MANET domain. MANETs have different characteristics from wired networks and even from standard wireless networks, there are new challenges related to security issues that need to be addressed.

The techniques used to handle Intrusion are Prevention, Detection and Tolerance.

R.S.Ambili Chandran is a M.Tech. student in Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, India. (email:ambily0123@gmail.com).

S. Mary Saira Bhanu is an Associate professor in the Department of Computer Science and Engineering, National Institute of Technology Tiruchirappalli, India.(email: msb@nitt.edu).

Prevention methods are inefficient in MANETs due to the unique features such as open nature, lack of infrastructure and central management, node mobility and dynamic topology. Various intrusion detection schemes were introduced to deal with the unique characteristics of MANETs. The schemes are either decentralized wherein all the nodes contain the intrusion detection module or centralized where a single node acts as a monitor.

Most of the Intrusion Detection System (IDS) works by manual intervention. When an intrusion is detected, the intrusion detection system will raise an alert and the user will react to the alert. This delay allows the intruder to access the information. For an intrusion detection scheme to be successful, it should act quickly before the intruder can access any information.

Intrusion tolerance is a design approach to defending information systems against malicious attack. Abandoning the conventional aim of preventing all intrusions, intrusion tolerance instead calls for triggering mechanisms that prevent intrusions from leading to a system security failure. The tolerance paradigm in security assumes that systems remain to a certain extent vulnerable and ensures that the overall system nevertheless remains secure and operational, with a measurable probability. Most of the intrusion tolerance schemes work with complex cryptographic algorithms. This will reduce the resource utilization which is a major factor in MANETs. So the intrusion tolerance scheme used should have better utilization of resources while it should also resist the intruder from getting into the system.

The response time of intrusion detection and tolerance is an important factor for the success of any intrusion detection system. In this paper, a context aware intrusion detection and tolerance at the application layer level is proposed to reduce the response time.

The rest of this paper is organized as follows. Section II discusses the previous work on context-aware intrusion detection and tolerance. The methodology used is explained in Section III. Section IV describes the proposed context-aware intrusion detection and tolerance architecture. The experimental results are discussed in Section V and Section VI is the conclusion.

II. RELATED WORK

There are several works regarding the context-aware intrusion detection system in ubiquitous computing environment. A generic architecting framework for adaptive context-aware intrusion detection system is proposed in [2]. They have suggested an intrusion tolerance which consists of a combination of intrusion detection and

DOI: 01.IJNS.01.03.52

a reaction step which is adaptable and concerns the runtime re-configuration of the deployed reaction policy together with the active monitors according to the context change. CoASec(Context Aware Security Management system) [3] enables management of context-aware security policies and enforcement of context-aware security services including user authentication and access control. CoASec security services are based on context-role based access control model and partial-credential based authentication management using the authentication credential value. The work in [4] has suggested that intrusion detection in mobile computing environment should be distributed and cooperative. The authors have also suggested that the analysis and anomaly detection should be done locally in each node and possibly through cooperation with all nodes in the network. A Service-oriented and User-centric Intrusion Detection System (SUIDS) for pervasive/ubiquitous computing is proposed in [5]. A Bayesian machine learning approach for spam filtering is proposed in [6]. In this approach a probability of validity is calculated for the incoming data from the history. The work in [7] is a context-aware peer to peer trust model for intrusion tolerance in MANETs is suggested. Some context-aware encryption techniques are suggested in [8].

III. METHODOLOGY USED

The methodology used is a distributed intrusion detection and reaction policy. All the nodes take part in the IDS and will try to detect intrusion with the help context-awareness. The monitor placing has a major role in intrusion detection since it has to consider the trade-off between the intrusion detection and the memory needed to store the policy repository. The IDS suggests an optimal monitor placement for MANETs. It will try to reduce the overhead of using more memory and at the same time maximize the detection of any threat in the system.

Whenever the IDS identify a node misusing resources in the network, it will be tolerated or denied access of the resources according to the context. The intrusion tolerance is done with the help of membership and proactive reaction measures which will reduce the response time of detection. The response time of detection can be improved in such architecture since the node can detect the intrusion directly. The problem in placing the IDS in each node is that in MANET, the resources are limited and thereby, each node may need more memory for placing the IDS. To reduce the consumption of memory at each node in the network a monitor can be selected among the nodes

The monitor is an intelligent one which learns and updates the database with the details about the nodes that have sent invalid data to the network. This information will be used for tolerating the nodes in the network according to the context.

.

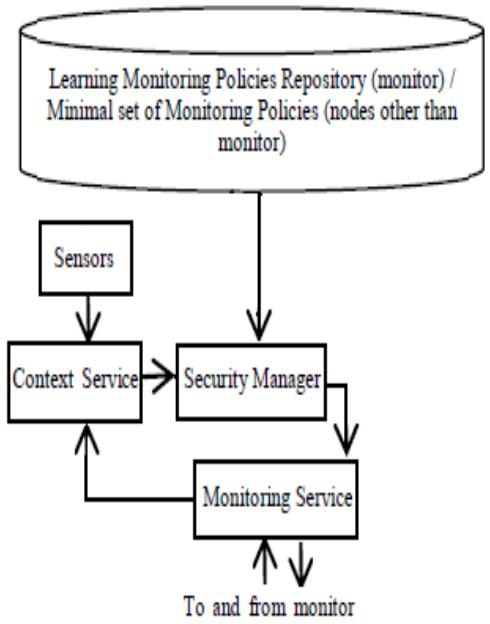

Fig. 1. Architecture framework for context-aware intrusion detection and tolerance

All the nodes in the network other than the monitor will be having a minimum level of filtering which will contain the minimum set of data to validate the messages, the membership details of the nodes and the details about the member nodes that are found to be working maliciously. The IDS proposed will try to minimize both the issues i.e., the response time and the utilization of the memory. The detection and tolerance scheme is based on the architecture proposed in [2].

IV. CONTEXT AWARE INTRUSION DETECTION AND TOLERANCE

The data flow in the architecture is as follows. The sensors will check the nodes present in the network and will send the information to the context service. The context service will analyze the data and will decide the context. The monitoring service will check the validity of the message by considering the policy specified for the context in the policy repository and will raise alerts in the case when it is not able to distinguish the validity of the message. The security manager manages the data flow between the repository, context service and the monitoring policy.

The entire network is divided into small areas and one of the nodes in the area is selected as the monitor. All the nodes other than the monitor will be having a minimum level of intrusion detection. Each of the nodes will be having a node membership database in it. If the sender is not a member, the data will be ignored. Otherwise, the data will be analyzed for the basic pattern which might be found in the message with the filtering in the destination. If the filtering fails, the message will be sent to the monitor for further analysis.

DOI: 01.IJNS.01.03.52

```
Message Received at destination
Check Destination is a monitor / non-monitor
If non-monitor
  Check the message using filtering
  If filtering succeeds
    Message accepted
  Else
    Message sent to the monitor in the region
  If monitor
    Check validity of message using Bayesian
      algorithm
    Update the database
    If message is invalidated by the monitor
      If the sender is an external member
        Value of invalid messages sent from the
          sender to the destination area is
          incremented
      If the value exceeds the threshold
        Internall member in the area is intimated
          about the intruder
        Internal nodes inside the area will store the
          node id of the intruder
```

Fig. 2. Algorithm for context-aware intrusion detection

The area for the monitor is considered by dividing the network as square areas and the node which is at the least distance from the centre of the square is considered as the monitor. So, the selected monitor will be the one which will be probably staying in the area for the maximum time. If the current monitor moves out of the area, a new monitor is selected using the same algorithm. The technique will reduce the average response time of the nodes using the minimum filter where as it will also reduce the total memory usage by placing the major IDS part in the monitor. The monitor will be having the same information as a normal node at the beginning. When the node is selected as a monitor, it will start learning and check the validity of messages using Bayesian learning algorithm. The monitor will also store the information about the nodes which are sending invalid messages. The algorithm for the intrusion detection is as shown in Fig 2.

```
Message Received at destination
Check Destination is a member/ non-
member
If sender is not a member
  Ignore the data
Else
  If member is listed as an intruder
    Message ignored
  Else
    Check for validity of message
```

Fig. 3. Algorithm for context-aware intrusion tolerance

Whenever a member node sends an invalid message to the monitor, (either for validating the message or for the monitor itself) the information in the message and the information about the sender node is saved in the monitor. If the sender member node is an external node, i.e., the location of the node is not in the similar service area as the receiver node, it will be tolerated to send message up to a threshold limit. When it exceeds the limit, then onwards, it will be considered as an intruder and the data send from that member node is ignored. If the sender member node is an internal node, i.e. it is located in the same service area as the receiver node, it will not be blocked. The algorithm for intrusion tolerance is as shown in Fig 3.

The main modules of the context-aware intrusion detection and tolerance system are as follows.

A. Monitor Placement

Selecting the monitor is done by checking the node's respective position in the network. Let "n" be the node and "nx" and "ny" be the x and y position of node. Let "X" and "Y" be the x and y coordinates of the centre position of the area considered. Then position of monitor node is calculated as: min [abs (X-nx) + abs(Y-ny)]

B. Node Types

There are mainly two types of node in an area.

- Filtering Node
- Monitoring node

Each region will have one monitor node and the rest of the nodes are filtering nodes.

C. Membership

All the nodes will have a list of nodes from which it will accept data. When a node which is not a member sends a message, the message will be ignored. The node which is a member can be an internal member or an external member. An internal member is a member that has the similar context data as of the current node (eg: if the current node is having the context of a university, the internal member will also have the same context). An external member is a member that is not in the similar context as of the current node.

DOI: 01.IJNS.01.03.52

D. *Bayesian Learning Algorithm*

Bayesian learning algorithm is used at the monitor for adapting to the context. The Bayesian algorithm is as shown in Fig 4.

```
ALL (No. of all messages) =
valid message count + invalid message count
P ("context data" | "message is invalid") =
for all matched word (invalid value of the current
context data/invalid message)
P ("context data" | "message is valid") =
for all matched word (valid value of
the current context data/valid message)
P ("message in invalid") =
invalid message count/Entire message count
P ("message is valid") =
valid message count/Entire message count
P ("message is invalid" | "context data") =
P ("message is invalid")
*P ("context data" | "message is invalid")
P ("message is valid" | "context data") =
P ("message is valid")
* P ("context data" | "message is valid")
Final result: P ("message is invalid" | "context data")
/P ("message is valid" | "context data")
```

Fig. 4. Bayesian Learning Algorithm for context-aware intrusion detection

V. EXPERIMENTAL RESULTS

The implementation of the IDS is done using simulator – GloMoSim and C#. The database used is My SQL. C# is used as a middle layer of communication between GloMoSim and My SQL. Database connectivity for implementing the Bayesian learning algorithm at the monitors is done with the help of C#. The nodes, messages sent between the nodes, the minimum filtering at the nodes and the monitor selection are simulated with the help of GloMoSim. The code of simulator is modified to implement intrusion detection and tolerance at the application layer. The application considered for simulation is FTP. The mobility of the nodes is according to random waypoint algorithm and the identification of the monitor is done at the random waypoint mobility generation.

Test Cases

The following test cases were considered for testing the implementation.

a. Sender node is not an internal or external member.
   In this case, the receiver which can be a monitor or a non-monitor node considers the sending node as an intruder.
b. Sender node is a member (internal / external) and receiving node is a non-monitor.
   In this case, the message will be checked for validity using the minimum filter at the receiving node and if filtering fails, message will be sent to the monitor for validation using the learning algorithm.
c. Sender node is a member (internal / external) and receiving node is a monitor.
   In this case, the message will be checked for validity using the learning algorithm.
d. Sender node is an external member and the receiving node is a monitor or a non-monitor. Also, the sending node sends invalid messages more than the threshold value to the nodes in a particular area and the receiver's position is in the same area.
   In this case, further messages from the corresponding external member node will be ignored.
e. Sender node is an internal member and the receiving node is a monitor or a non-monitor. Also, the sending node sends invalid messages more than the threshold value to the nodes in a particular area and the receiver's position is in the same area.
   In this case, further messages from the corresponding internal member node will not be ignored but tolerated.

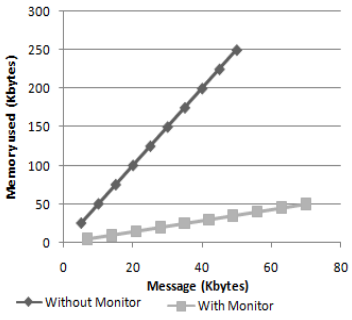

Fig. 5. Network overhead vs. memory overhead (with and without monitor)

The results of network overhead and memory used with and without monitor are shown in Fig. 5. The assumption is that five nodes are present and two messages among five messages are invalid of which one is resolvable at the node itself with the minimum filter.

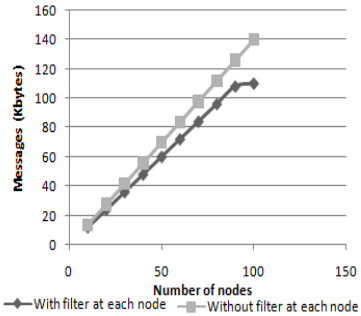

Fig. 6. Network overload with respect to number of nodes (with and without filter)

The results of network overhead with respect to the

DOI: 01.IJNS.01.03.52

increased number of nodes are shown in Fig. 6. It is assumed that two messages among ten messages will be invalid, of which one is resolvable at the node itself with the minimum filter.

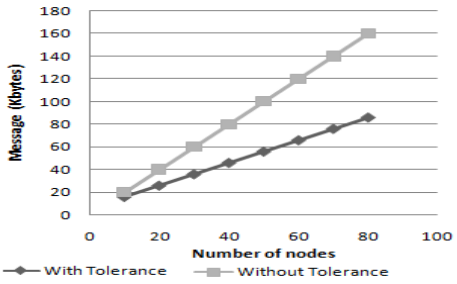

Fig. 7. Network overload vs. number of nodes (with and without tolerance)

The results of network overhead with respect to the increased number of nodes are shown in Fig. 7. It is assumed that five messages among ten messages sent from an external member will be invalid, of which none is resolvable at the node itself with the minimum filter.

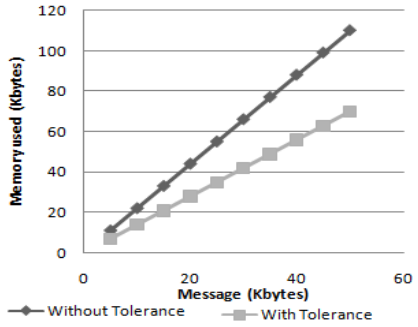

Fig. 8. Network overhead vs. memory overhead (with and without tolerance)

The results of network overhead and memory used with and without tolerance are shown in Fig. 8. The assumption is that five nodes are present and three messages among five messages are invalid and the threshold is one invalid message.

VI. CONCLUSION

A context aware intrusion detection and tolerance technique for MANETs suggested in this paper is adaptive to the context. Intrusion detection is distributed and reaction policy is used. The tolerance is done proactively by sending the intruder data to the members. This will reduce the chances of resources from getting overloaded by the intruders. Also, the proactive scheme will help to reduce the number of messages being transmitted in the network. Thus this algorithm will provide improved utilization of resources which is very sensitive in the case of MANETs.

REFERENCES

[1] R. S. Ambili Chandran and S. Mary Saira Bhanu, "Context-Aware Intrusion Detection in Mobile Ad-Hoc Networks", V.V Das et al. (Eds): BAIP 2010, CCTS 70, pp, 458-460, 2010, Springer-Verlag Berlin Heidelberg 2010

[2] Ayda Saidane "A Reliable Context-Aware Intrusion Tolerant System" R.Meersman,Z.Tari, P. Herrero et al. (Eds.):OTM 2007 Ws, Part II,LNCS 4806, pp. 1062–1070, 2007. Springer-*Verlag Berlin Heidelberg*

[3] *Seon-Ho Park, Joon*-Sic Cho, Young-Ju Han, and Tai-Myoung Chung "Design and Implementation of Context-Aware Security Management System for Ubiquitous Computing Environment" P. Thulasiraman et al. (Eds.): ISPA 2007 Workshops, LNCS 4743, pp. 235–244, 2007. Springer-Verlag Berlin Heidelberg

[4] Zhang Y, Lee W, Huang Y "Intrusion detection techniques for mobile wireless networks", 2003, A CM MONET Journal pages 3

[5] Zhou B, Shi Q, Merabti M "Intrusion Detection in Pervasive Networks Based on a Chi-Square Statistic Test" In: Computer Software and Applications Conference, 2006. COMPSAC 2006. 30th Annual International pages 3

[6] Sahami M, Dumais S, Heckerman D, Horvitz E "A Bayesian Approach to Filtering Junk E-Mail", 1998, AAAI'98 Workshop on Learning for Text Categorization, 1998

[7] Shankaran R, Varadharajan V, Orgun M A, and Hitchens M "Context-Aware Trust Management for Peer-to-Peer Mobile Ad-Hoc Networks", 33rd Annual IEEE International Computer Software and Applications Conference 2009

[8] Lyndon G Pierson, Edward L Witzke,Mark O Bean, Gerry J Trombley "Context-Agile Encryption for High Speed Communication Networks" ACM SIGCOMM Computer Communication Review 1999

[9] Jalal Al-Muhtadi, Raquel Hill, Roy Campbell, Dennis Mickunas M "Context and Location-Aware Encryption for Pervasive Computing Environments" Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops 2006

DOI: 01.IJNS.01.03.52